TD 7 : corrigé

2. Facteurs directs et projecteurs

1. Le raisonnement est assez similaire à la preuve que dans un espace vectoriel, un projecteur, c'est-à-dire un endomorphisme $\pi : \mathrm{E} \to \mathrm{E}$ vérifiant $\pi_{|\mathrm{im}\,\pi} = \mathrm{id}_{\mathrm{im}\,\pi}$ donne naissance à une décomposition en somme directe $\mathrm{E} = \ker(\pi - \mathrm{id}_\mathrm{E}) \oplus \ker\pi$.

Supposons donc, pour commencer, que tout élément m du A-module M se décompose de manière unique en $m = n + p$ avec $n \in \mathrm{N}$ et $p \in \mathrm{P}$. On peut alors définir une application

$$\pi : \begin{array}{ccc} \mathrm{M} & \to & \mathrm{N} \\ m & \mapsto & n \end{array}.$$

Cette application est alors un morphisme de A-modules (on parle aussi *d'application* A-*linéaire*) : soit $a \in \mathrm{A}$ et $m_1, m_2 \in \mathrm{M}$. On décompose les deux éléments m_i en $m_i = n_i + p_i$, avec $n_i \in \mathrm{N}$ et $p_i \in \mathrm{P}$. L'écriture $m_1 + a m_2 = (n_1 + a n_2) + (p_1 + a p_2)$, qui vérifie bien $n_1 + a n_2 \in \mathrm{N}$ et $p_1 + a p_2 \in \mathrm{P}$, démontre alors que $\pi(m_1 + a m_2) = n_1 + a n_2 = \pi(m_1) + a\pi(m_2)$. Par définition, π vaut l'identité en restriction à N et on a bien construit le morphisme désiré.

Réciproquement, si $\pi : \mathrm{M} \to \mathrm{N}$ est A-linéaire et vérifie $\pi_{|\mathrm{N}} = \mathrm{id}_\mathrm{N}$, posons

$$\mathrm{P} = \mathrm{im}(\mathrm{id}_\mathrm{M} - \pi) = \left\{ m - \pi(m) \,\middle|\, m \in \mathrm{M} \right\}.$$

Puisque $\mathrm{id}_\mathrm{M} - \pi$ est un morphisme de A-modules, P est bien un sous-module de M. L'existence d'une décomposition résulte de l'expression suivante, valable pour tout $m \in \mathrm{M}$:

$$m = \underbrace{\pi(m)}_{\in \mathrm{N}} + \underbrace{m - \pi(m)}_{\in \mathrm{P}}.$$

Il ne reste plus qu'à en montrer l'unicité. Pour cela, commençons par remarquer que π est bien un projecteur, c'est-à-dire que $\pi^2 = \pi$ (cela provient du fait que pour tout $m \in \mathrm{M}$, $\pi(m) \in \mathrm{N}$ et que π restreint à N vaut l'identité). Puisque tout élément de P s'écrit $m - \pi(m)$ pour un certain $m \in \mathrm{M}$, on a donc $\pi(m - \pi(m)) = \pi(m) - \pi^2(m) = 0$, c'est-à-dire $\mathrm{P} \subset \ker\pi$. Prenons maintenant deux décompositions d'un même élément $m = n + p = n' + p'$, avec $n, n' \in \mathrm{N}$ et $p, p' \in \mathrm{P}$. On a alors $n - n' = p' - p \in \mathrm{N} \cap \mathrm{P}$. L'unicité de la décomposition résultera donc de $\mathrm{N} \cap \mathrm{P} = \{0\}$, qui est facile à vérifier : si $x \in \mathrm{N} \cap \mathrm{P}$, on a à la fois $\pi(x) = x$ et, d'après ce qui précède, $\pi(x) = 0$, d'où $x = 0$.

2. D'après la première question, si $2\mathbb{Z}$ était un facteur direct de $\mathbb{Z}$, on pourrait trouver un morphisme de $\mathbb{Z}$-modules $\pi : \mathbb{Z} \to 2\mathbb{Z}$ valant l'identité en restriction à $2\mathbb{Z}$. On aurait donc notamment (par $\mathbb{Z}$-linéarité) :

$$2 = \pi(2) = 2\pi(1),$$

ce qui implique $\pi(1) = 1 \notin 2\mathbb{Z}$ et constitue une contradiction.

Remarque : Une autre preuve consiste à dire que l'on connaît bien les sous-$\mathbb{Z}$-modules de $\mathbb{Z}$: ce sont les $a\mathbb{Z}$, pour les divers choix de $a \in \mathbb{Z}$. On vérifie en effet facilement que ce sont

des sous-modules, et l'on a déjà vu que ce sont les seuls, puisque ce sont déjà les seuls sous-groupes additifs de $\mathbb{Z}$. Pour que $2\mathbb{Z}$ soit un facteur direct, il faudrait alors qu'un autre sous-module de $\mathbb{Z}$ soit « en somme directe » avec $2\mathbb{Z}$, au sens où une unique décomposition existe. Mais cela est impossible car $2\mathbb{Z}$ rencontre non trivialement tous les $a\mathbb{Z}$ dès que a est non nul.

5. Relation de Bézout et théorème chinois

1. Déjà, rappelons que « l'application naturelle » dont parle l'énoncé est

$$\varphi : \begin{array}{ccc} \mathbb{Z}/ab\mathbb{Z} & \to & \mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z} \\ [x]_{ab} & \mapsto & ([x]_a,[x]_b) \end{array},$$

où l'on décide de noter $[x]_n$ la classe modulo n d'un entier x. Il est facile de voir que cette application est bien définie, et le théorème chinois affirme précisément que c'est même un isomorphisme d'anneaux.

Pour en trouver une réciproque, écrivons une relation de Bézout

$$au+bv=1$$

liant a et b. Notons que cela implique que au est congru à 1 modulo b, et bv congru à 1 modulo a. Puisqu'il est évident qu'ils sont en outre congrus à 0 modulo a et b respectivement, l'entier $auz+bvy$ est alors congru à x modulo a et à y modulo b et sa classe modulo ab est bien définie (on peut le vérifier à la main mais, puisque l'on connaît sa classe modulo a et sa classe modulo b, c'est également une conséquence du théorème chinois).

L'application

$$\begin{array}{ccc} \mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z} & \to & \mathbb{Z}/ab\mathbb{Z} \\ ([y]_a,[z]_b) & \mapsto & [auz+bvy]_{ab} \end{array}$$

est alors la réciproque recherchée.

2. Le théorème chinois va nous permettre de traduire ce problème modulo 35 en deux problèmes, l'un modulo 5 et l'autre modulo 7. En effet, un entier x vérifie $x^2\equiv 9 \mod 35$ si et seulement si x^2 est congru à 9 modulo 5 et modulo 7. En testant toutes les possibilités (ou la moitié des possibilités si on se souvient que $(-x)^2=x^2$), on montre facilement que les seules racines de 9 sont 2 et $3=-2$ modulo 5 et 3 et $4=-3$ modulo 7. On peut alors exploiter une relation de Bézout liant 5 et 7, par exemple

$$3\times 7-4\times 5=1$$

pour obtenir, grâce à la question précédente, les solutions modulo 35.

$[x]_5$	$[y]_7$	$[21x-20y]_{35}$
$[2]_5$	$[3]_7$	$[17]_{35}$
$[3]_5$	$[4]_7$	$[18]_{35}$
$[3]_5$	$[3]_7$	$[3]_{35}$
$[2]_5$	$[4]_7$	$[32]_{35}$

La première et la deuxième ligne d'une part, et d'autre part la troisième et la quatrième sont constituées de classes opposées (puisque l'on a $\varphi([-x]_{ab})=([-x]_a,[-x]_b)$).

Au final, *les entiers dont le carré est congru à 9 modulo 35 sont exactement les entiers congrus à 3, 17, 18 ou 32 modulo 35.*

6. Quotient et idéal

1. Commençons par démontrer un résultat d'intérêt général.

Lemme.
Soit A *et* B *deux anneaux et* $f : \mathrm{A} \to \mathrm{B}$ *un morphisme. On note* $\mathrm{I} = \ker f \lhd \mathrm{A}$. *Alors :*
- *Si* J *est un idéal de* B, $f^{-1}[\mathrm{J}]$ *est un idéal de* A.
- *Si* f *est surjectif et que* J *est un idéal de* A, $f[\mathrm{J}]$ *est un idéal de* B.

Preuve : Il est d'abord évident que dans les deux cas, l'ensemble considéré est bien un sous-groupe additif du groupe additif de l'anneau. Il ne reste qu'à démontrer la propriété multiplicative.

Soit donc, dans le cadre du premier point, $a \in \mathrm{A}$ et $x \in f^{-1}[\mathrm{J}]$. On a $f(ax) = f(a)f(x)$. $f(x)$ appartient par définition à l'idéal J, donc $f(ax) \in \mathrm{J}$ et $ax \in f^{-1}[\mathrm{J}]$.

Parallèlement, avec les notations du deuxième point, soit $b \in \mathrm{B}$ et $y \in f[\mathrm{J}]$. On écrit $y = f(x)$, avec $x \in \mathrm{J}$. Par surjectivité de f, on peut trouver $a \in \mathrm{A}$ tel que $b = f(a)$. On a alors bien $by = f(ax) \in f[\mathrm{J}]$, car $ax \in \mathrm{J}$. □

Si on a un anneau A et un idéal I, le lemme nous fournit donc un billet aller-retour entre les idéaux de A et ceux de A/I : il suffit de prendre leur image (directe ou réciproque, suivant le cas) par la projection $\pi : \mathrm{A} \to \mathrm{A/I}$.

Quelle que soit la partie F de A/I, la surjectivité de π prouve que $\pi[\pi^{-1}[\mathrm{F}]] = \mathrm{F}$. L'opération « image réciproque par π » est donc un inverse à gauche de l'opération « image directe ».

Pour un idéal J de A, $\pi^{-1}[\pi[\mathrm{J}]]$ est l'idéal de A formé des éléments $x \in \mathrm{A}$ qui ont la même image par π qu'un élément j de J. La différence $i - j$ appartient donc à $\ker \pi = \mathrm{I}$. L'inclusion réciproque étant immédiate, on a $\pi^{-1}[\pi[\mathrm{J}]] = \mathrm{I} + \mathrm{J}$.

En particulier, si on se restreint aux idéaux J de A *contenant* I (et donc tels que $\mathrm{I} + \mathrm{J} = \mathrm{J}$), les images directe et réciproque par I fournissent des bijections réciproques :

$$\{\text{idéaux de A contenant I}\} \simeq \{\text{idéaux de A/I}\}.$$

En outre, si J est un idéal de A contenant I, la projection $p : \mathrm{A} \to \mathrm{A/(I+J)}$ possède I dans son noyau, donc elle se factorise, par le théorème d'isomorphisme, en $p : \mathrm{A} \xrightarrow{\pi} \mathrm{A/I} \xrightarrow{\overline{p}} \mathrm{A/J}$. Toutes les flèches étant surjectives, on a $\mathrm{J} = \ker p$ et $\pi[\mathrm{J}] = \ker \overline{p}$. Le théorème d'isomorphisme prouve que les anneaux quotients (A/I)/J et $\mathrm{A}/\pi[\mathrm{J}]$ sont isomorphes. Ils sont donc intègres (resp. des corps) simultanément, ce qui prouve que J est un idéal premier (resp. maximal) de A exactement quand $\pi[\mathrm{J}]$ est un idéal premier (resp. maximal) de A/I.

2. Convenons de noter $[a]_{\mathrm{L}}$ la classe de $a \in \mathrm{A}$ dans l'anneau quotient A/L pour un idéal quelconque L de A. On a alors une application bien définie $\pi : \begin{array}{ccc} \mathrm{A/I} & \to & \mathrm{A/(I+J)} \\ [x]_{\mathrm{I}} & \mapsto & [x]_{\mathrm{I+J}} \end{array}$ dont il est facile de voir que c'est un morphisme d'anneaux surjectif. Cela démontre que $\mathrm{A/(I+J)}$ peut être vu comme un quotient de A/I. Montrons que le noyau de ce morphisme est l'idéal $\overline{\mathrm{J}}$ qui est l'image de $\mathrm{I} + \mathrm{J}$ (ou de J) par la surjection canonique $\mathrm{A} \mapsto \mathrm{A/I}$, c'est-à-dire

$$\overline{\mathrm{J}} = \left\{ [x]_{\mathrm{I}} \,\middle|\, x \in \mathrm{I} + \mathrm{J} \right\}.$$

Tout d'abord si $x \in \mathrm{I} + \mathrm{J}$, $[x]_{\mathrm{I+J}} = 0$, donc $[x]_{\mathrm{I}} \in \ker \pi$. Réciproquement, si $\xi \in \ker \pi$, on peut écrire $\xi = [x]_{\mathrm{I}}$ pour un certain $x \in \mathrm{A}$. Il vérifiera alors que $\pi(\xi) = \pi([x]_{\mathrm{I}}) = [x]_{\mathrm{I+J}}$.

On a donc un isomorphisme :

$$(\mathrm{A}/\mathrm{I})/\overline{\mathrm{J}} \simeq \mathrm{A}/(\mathrm{I}+\mathrm{J}).$$

NB : En particulier, cela donne, dans le cas où $\mathrm{I}=(x)$ et $\mathrm{J}=(y)$ sont des idéaux principaux : $\mathrm{A}/(x,y)=(\mathrm{A}/(x))/(\overline{y})=(\mathrm{A}/(y))/(\overline{x})$, où $\overline{x}$ et $\overline{y}$ sont respectivement l'image de x dans $\mathrm{A}/(y)$ et celle de y dans $\mathrm{A}/(x)$.

3. On a déjà vu dans le lemme que si $\varphi : \mathrm{A} \to \mathrm{B}$ est surjectif, il envoie tout idéal de A sur un idéal de B. En fait, la réciproque est également vraie : si φ possède cette propriété, $\varphi[\mathrm{A}]$ est un idéal de B contenant $\varphi(1_\mathrm{A})=1_\mathrm{B}$, donc $\varphi[\mathrm{A}]=\mathrm{B}$ et φ est surjectif.

8. Idéaux premiers et maximaux des anneaux principaux

Soit A un anneau commutatif.

Une remarque importante pour commencer est qu'une décomposition d'un élément non nul $x \in \mathrm{A}\setminus\{0\}$ en produit $x=ab$ fournit une suite d'inclusion d'idéaux de A :

$$(x) \subset (a) \subset \mathrm{A}.$$

Réciproquement, une inclusion $(x)\subset(a)$ garantit qu'il existe $b\in\mathrm{A}$ tel que $x=ab$.

La première inclusion $(x)\subset(a)$ est stricte si et seulement si b n'est pas inversible : si b est inversible, x et a sont conjugués et engendrent donc le même idéal, c'est-à-dire $(x)=(a)$; réciproquement, si $(x)=(a)$, on peut écrire $a=kx$ pour un certain $k\in\mathrm{A}$, ce qui implique $x=bkx$, d'où $x(bk-1)=0$ et, par intégrité de A (un anneau principal est intègre, par définition !), $bk=1$ et $b\in\mathrm{A}^\times$.

La seconde inclusion $(a)\subset\mathrm{A}$ est quant à elle stricte si et seulement si a n'est pas inversible.

Mises bout à bout, ces remarques impliquent un résultat partiel intéressant, valable pour tous les anneaux commutatifs : *un élément non nul x est irréductible si et seulement si l'idéal qu'il engendre est maximal* ***parmi les idéaux principaux***.

Si l'on suppose maintenant A principal, tous les idéaux sont principaux et le résultat précédent implique que, pour x non nul, (x) est un idéal maximal si et seulement si x est irréductible. Puisque maximal implique premier (un corps est intègre !), ces idéaux sont également premiers. L'idéal nul, quant à lui, est premier ($\mathrm{A}=\mathrm{A}/\{0\}$ est principal, donc intègre), mais pas maximal (on a supposé que A n'était pas un corps).

Pour terminer l'exercice, il faut montrer que si x n'est ni nul ni irréductible, l'idéal (x) n'est pas seulement non maximal, mais il est aussi non premier. Pour cela, soit $x=ab$ une décomposition non triviale, c'est-à-dire que ni a ni b n'est inversible. On a alors $ab\in(x)$ mais ni a ni b n'appartiennent à (x) : si on avait $a\in(x)$, on aurait $(a)=(x)$ et, comme plus haut, b serait inversible.

Remarque : L'hypothèse de principalité est primordiale dans cet exercice : en général, les idéaux premiers sont beaucoup plus nombreux que les idéaux maximaux. Par exemple, si $\mathrm{A}=\mathbb{C}[\mathrm{X},\mathrm{Y}]$, on peut démontrer que les seuls idéaux maximaux de A sont les $(\mathrm{X}-x_0,\mathrm{Y}-y_0)$ avec $(x_0,y_0)\in\mathbb{C}^2$, dont les quotients sont simplement les applications « d'évaluation » :

$$\begin{array}{rccc} \text{év}_{(x_0,y_0)}: & \mathbb{C}[\mathrm{X},\mathrm{Y}] & \to & \mathbb{C}[\mathrm{X},\mathrm{Y}]/(\mathrm{X}-x_0,\mathrm{Y}-y_0)\simeq\mathbb{C} \\ & \mathrm{P} & \mapsto & \mathrm{P}(x_0,y_0) \end{array}.$$

À côté de ces idéaux maximaux correspondant aux points (x_0, y_0) de $\mathbb{C}^2$, il y a beaucoup d'idéaux premiers correspondant à des « courbes », comme par exemple $\mathrm{I}_{axe\ horizontal} = (\mathrm{Y})$, de quotient $\mathbb{C}[\mathrm{X},\mathrm{Y}]/(\mathrm{Y}) \simeq \mathbb{C}[\mathrm{X}]$, ou encore $\mathrm{I}_{cercle} = (\mathrm{X}^2 + \mathrm{Y}^2 - 1)$...

12. Entiers de Gauß

1. Le module d'un nombre complexe est déjà une application multiplicative de $\mathbb{C}$ dans $\mathbb{R}_+^*$. Cela reste donc vrai pour le module au carré, restreint aux entiers de Gauß (et l'image est bien dans ce cas incluse dans $\mathbb{N}$.)

2. D'après la question précédente, un inversible $z \in \mathbb{Z}[i]^\times$ vérifie $\mathrm{N}(z) \in \mathbb{N} \cap \mathbb{Z}^\times : \mathrm{N}(z) = 1$. On a donc $z \in \{\pm 1, \pm i\}$ et il est évident que ces quatre nombres complexes conviennent.

$$\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}.$$

3. Montrons cette équivalence, portant sur $a \in \mathbb{Z}[i]$ et $b \in \mathbb{Z}[i] \setminus \{0\}$:

$$\begin{aligned}
\exists q, r \in \mathbb{Z}[i] : a = bq + r \text{ et } \mathrm{N}(r) < \mathrm{N}(b) &\iff \exists q, r \in \mathbb{Z}[i] : \frac{a}{b} = q + \frac{r}{b} \text{ et } \mathrm{N}\left(\frac{r}{b}\right) < 1 \\
&\iff \exists q, r \in \mathbb{Z}[i] : \frac{a}{b} - q = \frac{r}{b} \text{ et } \left|\frac{r}{b}\right| < 1 \\
&\iff \exists q \in \mathbb{Z}[i] : \left|\frac{a}{b} - q\right| < 1
\end{aligned}$$

4. On va démontrer que $\mathbb{Z}[i]$ est euclidien avec N comme stathme. C'est exactement la première proposition de la question précédente. Il suffit donc de montrer que pour tous éléments a et b dans $\mathbb{Z}[i]$, b non nul, $\dfrac{a}{b}$ est à distance inférieure à 1 d'un entier de Gauß. Or, tout nombre complexe z est à distance inférieure à 1 d'un entier de Gauß : si x_0 est l'entier le plus proche de $\mathrm{Ré}\, z$ et y_0 l'entier le plus proche de $\mathrm{Im}\, z$, $|z - (x_0 + i y_0)| \leqslant \dfrac{\sqrt{2}}{2} < 1$. $\mathbb{Z}[i]$ est donc euclidien.

5. L'équivalence de la question 4 nous fournit une manière explicite de faire le calcul de la division euclidienne, et on peut donc appliquer l'algorithme d'Euclide. $(3+i)/(1+3i) = 3/5 - 4/5i$ est à distance < 1 de l'entier de Gauss $1 - i$. On a donc une division euclidienne avec un quotient égal à $1 + i$ et un reste que l'on calcule aisément :

$$3 + i = (1 + 3i) \cdot (1 - i) - (1 + i).$$

L'étape suivante du calcul « tombe juste » (on peut oublier le signe du reste, puisque -1 est inversible) :

$$(1 + 3i) = (1 + i) \cdot (2 + i).$$

On a donc $(3 + i, 1 + 3i) = (1 + 3i, 1 + i) = (1 + i)$. Le pgcd de $3 + i$ et $1 + 3i$ dans $\mathbb{Z}[i]$ est donc (à un inversible près) $1 + i$.

On peut comme à l'accoutumée « remonter » l'algorithme d'Euclide pour obtenir une relation de Bézout :

$$1 + i = (1 + 3i) \cdot (1 - i) - (3 + i) \cdot 1.$$